UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

NAGRAVISION SA,	§	Case No.
	§	
Plaintiff,	§	
	§	
vs.	§	
	§	
DOES 1-7,	§	
	§	
Defendants.	§	

PLAINTIFF NAGRAVISION'S MEMORANDUM IN SUPPORT OF MOTION FOR LEAVE TO CONDUCT EXPEDITED DISCOVERY

Plaintiff Nagravision SA ("Nagravision") respectfully files this memorandum in support of its motion for leave to conduct limited discovery prior to the Federal Rule of Civil Procedure 26(f) conference for the purpose of identifying Defendant Does 1-7.

I. FACTUAL BACKGROUND

Nagravision brings this action against Defendant Does 1-7 ("Defendants") based on their operation of multiple computer servers that illegally retransmit Nagravision's control words and thereby enable countless end users to circumvent Nagravision's security technology and receive the copyrighted television programming provided by Nagravision's customer without paying the required subscription fee. As explained below, Defendants have not been identified other than by the IP addresses of the computer servers that are used in their piracy operation, and thus subpoenas to the Internet Service Providers or "ISPs" are needed to uncover Defendants' true identities.

A. Nagravision's Security Technology

Several leading broadcasters in the pay-television industry employ Nagravision's security technology to provide secure access to their subscription-based television services. (Declaration of Pascal Metral ¶ 3.) Nagravision's customers include DISH Network in the United States, Bell TV in Canada, Canal+ in France, and other major pay-television broadcasters in North America, South America, Europe, and Asia. (*Id.*)

Pay-television broadcasters that implement the Nagravision security technology transmit their signal to subscribers in an encrypted form. (*Id.* ¶ 4.) In order to receive the signal, subscribers must purchase or lease from the broadcaster a receiver paired with a smart card and a programming subscription plan. (*Id.*) Viewing rights vary based on the services the subscriber purchased from the pay-television broadcaster. (*Id.*)

Nagravision designs and licenses software that is incorporated into the receivers and smart cards, and also manufactures smart cards. (*Id.* ¶ 5.) The smart card is used to (i) manage, store, and communicate to the receiver the subscriber's right to decrypt specific channels based on his subscription plan, and (ii) decrypt the encrypted control words or "keys" required to unlock and view the channels for which the subscriber purchased access. (*Id.*)

Nagravision's control words are transmitted to subscribers as part of the encrypted audio and video streams of the pay-television broadcaster. (*Id.* ¶ 6.) Control words are channel specific and change approximately every five to ten seconds for a given channel. (*Id.*) Control words are double protected by being delivered in encrypted packets called "entitlement control messages" or "ECMs." (*Id.*) The keys used to decrypt these ECMs, called "transmission keys," are stored in the memory of the subscriber's smart card and may be changed by the pay-television broadcaster over the air as needed. (*Id.*)

When a subscriber wants to view a specific pay-television channel, the receiver obtains the ECM containing the encrypted control word from the satellite stream and forwards it to the smart card. (*Id.* ¶ 7.) The smart card uses its current transmission key to decrypt the ECM. (*Id.*) The smart card then checks its rights database to confirm that the subscriber purchased a subscription to view the programming the control word will decrypt. (*Id.*) If the rights match, the smart card forwards the unencrypted control word to the receiver, where the control word decrypts the pay-television broadcast. (*Id.*) In this way, the Nagravision security technology plays a vital role in ensuring its customers' television programming is made accessible only to authorized subscribers that have purchased the right to view the content. (*Id.*)

B. Defendants' Unlawful Circumvention of Nagravision's Security Technology

"Internet key sharing" or "IKS" is a form of pay-television piracy that centers around the unauthorized harvesting and redistribution of Nagravision's control words. (*Id.* ¶ 8.) The control words are obtained by purchasing a subscription with a pay-television broadcaster, and then using a genuine smart card activated on that subscription account to decrypt ECMs containing the control words. (*Id.*) Once decrypted, the control words are sent from the smart card to a computer server, called an "IKS server," where the control words are saved in the server's memory or cache. (*Id.*)

Nagravision's control words are retransmitted from the IKS server to end users. (*Id.* ¶ 9.) End users access the IKS server with an unauthorized receiver connected to the Internet. (*Id.*) When the end user tunes to a pay-television channel, the unauthorized receiver requests the control word for that particular channel from the IKS server. (*Id.*) The IKS server sends the control word over the Internet to the unauthorized receiver, enabling the end user to decrypt the channel without having authorization from and without making payment to the pay-television broadcaster. (*Id.*)

Defendants are running an IKS service through the use of at least 7 servers in the United States, 4 of which are located in Texas. (*Id.* ¶¶ 10-11.) Nagravision identified the servers through IP tracing, whereby Nagravision connected an unauthorized receiver to the IKS service and using a network analysis tool was able to identify the IP addresses of the servers accessed by the receiver in the course of obtaining Nagravision's control words, or by analyzing network traffic to and from other servers that were part of the IKS service supporting some of the same unauthorized receivers. (*Id.* ¶ 10.) The servers identified by Nagravision functioned as a cache by storing Nagravision's control words, and a front end by retransmitting the control words from the cache to end users that request them through their unauthorized receiver. (*Id.* ¶ 11.)

The following chart has the IP addresses of control word servers identified by Nagravision, the unauthorized receiver supported by the servers, the ISP to which the IP address was assigned according to publicly available Whois data, and the geolocation of the IP address:

IP Address	Reference Name	Unauthorized Receiver Supported By Server	ISP Name & Server Location
208.98.21.253	CW Server 1	Magnum MR-9800S	Sharktech, Inc. Chicago, Illinois
174.128.224.202	CW Server 2	Geant GN-2000HD	Sharktech, Inc. Denver, Colorado
192.151.156.122	CW Server 3	Atlas HD-200S	DataShack, LC North Kansas City, Missouri
45.34.7.202	CW Server 4	Atlas HD-200S/200Se	Psychz Networks Dallas, Texas
45.35.61.10	CW Server 5	Atlas HD-200S/200Se	Psychz Networks Dallas, Texas
45.35.70.202	CW Server 6	Atlas HD-200S/200Se	Psychz Networks Dallas, Texas
45.34.7.82	CW Server 7	Atlas HD-100	Psychz Networks Dallas, Texas

(*Id.* ¶ 11, Exs. 1-14.) CW Servers 1-7 are used to provide Nagravision's control words to Magnum, Geant, and Atlas receivers, which in turn enable the end user to circumvent Nagravision's security technology and receive without authorization the subscription-based television programming of Nagravision's customer, Canal+. (*Id.* ¶ 12, Exs. 15-17.)

The ISPs identified in the chart above – Sharktech, DataShack, and Pyschz Networks – are expected to have information identifying their customers that are responsible for CW Servers 1-7, i.e., Does 1-7, and therefore are the intended recipients of Nagravision's subpoenas. (*Id.* ¶ 13.)

II. LEGAL STANDARD

Discovery may be conducted prior to the Rule 26(f) conference when authorized by court order. Fed. R. Civ. P. 26(d)(1). District courts in the Fifth Circuit have adopted a "good cause" standard to determine whether to permit expedited discovery. *See, e.g., St. Louis Group, Inc. v. Metals & Additives Corp.*, 275 F.R.D. 236, 239-40 (S.D. Tex. 2011) (citing cases); *Turner Indus. Group, Inc. v. Int'l Union of Operating Eng'rs, Local 450*, No. H-13-0456, 2013 WL 2147515, at *3 (S.D. Tex. May 10, 2013). "Good cause exists 'where the need for expedited discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party'." *Turner*, 2013 WL 2147515, at *3 (quoting *St. Louis Group*).

When considering requests for expedited discovery to identify anonymous Internet users, courts have taken into account: "(1) whether the plaintiff makes a prima facie showing of harm; (2) the specificity of the discovery request; (3) the absence of alternative means to obtain the subpoenaed information; (4) the necessity of the subpoenaed information to advance the claim; and (5) the user's expectation of privacy." *Id.*; *Well Go USA, Inc. v. Unknown Participants in Filesharing Swarm Identified By Hash: B7FEC872874DoCC9B1372ECE5ED07AD7420A3BBB*, No. 4:12-cv-00963, 2012 WL 4387420, at *1 (S.D. Tex. Sept. 25, 2012); *Indigital Sols., LLC v. Mohammed*, No. H-12-2428, 2012 WL 5825824, at *2 (S.D. Tex. Nov. 15, 2012); *Combat Zone Corp. v. Does 1-13*, No. 3:12-CV-3927-B, 2013 WL 230382, at *4 (N.D. Tex. Jan 22, 2013). Consideration of the foregoing factors demonstrates that there is good cause to grant Nagravision's request for expedited discovery.

III. ARGUMENT

A. Nagravision States A Prima Facie Claim Of Actionable Harm Against Defendants

Nagravision states a claim against Defendants under the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2) ("DMCA"). (Compl. ¶¶ 19-24.) The DMCA makes it unlawful to offer to the public, provide, or otherwise traffic in any technology, product, service, or part thereof that satisfies one of three criteria: (1) it is primarily designed or produced for circumventing a measure that effectively controls access to a copyrighted work; (2) it has only limited commercial purpose or use other than circumventing such a measure; or (3) it is marketed by the defendant or another acting in concert for use in circumventing such a measure. 17 U.S.C. § 1201(a)(2). To circumvent an access control measure "means to descramble a scrambled work, to decrypt an encrypted work, or to otherwise avoid, bypass, remove, deactivate, or impair a technological measure." *Id.* § 1201(a)(3)(A).

Nagravision's encryption-based security technology is an effective access control measure for purposes of the DMCA. *See, e.g., DISH Network L.L.C. v. Sonicview USA, Inc.*, No. 09-cv-1553-L(WVG), 2012 WL 1965279, at *8 (S.D. Cal. May 31, 2012); *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000) (holding that security measures based on

"encryption or scrambling" are deemed effective for purposes of the DMCA). And, Nagravision has standing to assert a DMCA claim against persons that are circumventing its security measures. *See* 17 U.S.C. § 1203(a) (authorizing a civil claim by "[a]ny person injured by a violation of section 1201"); *Bose BV v. Zavala*, No. 09-11360-GAO, 2010 WL 152072, at *2 (D. Mass. Jan. 14, 2010) ("A party who controls the technological measures that protect copyrighted works has routinely been deemed a 'person injured' by the circumvention of these measures.").

Nagravision pleads a prima facie claim under the DMCA by alleging that Defendants are operating an IKS service through the use of servers in the United States, including CW Servers 1-7. (Compl. ¶¶ 14-15.) Defendants' IKS service is used to retransmit Nagravision's control words to end users, thereby enabling them to circumvent Nagravision's security technology and receive television programming provided by Nagravision's customer, Canal+, without paying the required subscription fee. (*Id.* ¶¶ 16-17.) Defendants' IKS service, and the underlying control word sharing technology, was designed and produced for circumventing Nagravision's security technology and has no legitimate commercial purpose or use. (*Id.* ¶ 21.) By providing this IKS service and control work sharing technology, Defendants are violating section 1201(a)(2) of the DMCA. (*Id.* ¶ 20.)

In summary, Nagravision states a prima facie claim of actionable harm under the DMCA. *See Nagravision SA v. Zhuhai Gotech Intelligent Tech. Co.*, No. 4:15-cv-00403, Dkt. 29 (S.D. Tex. Aug. 18, 2016) (entering default judgment and permanent injunction for Nagravision upon finding allegations that defendants operated an IKS service from servers in the United States stated a claim for relief under the DMCA) (attached at Metral Decl. Ex. 19); *DISH Network L.L.C. v. Ramirez*, No. 15-cv-04712-BLF, 2016 WL 3092184, at *3 (N.D. Cal. June 2, 2016) (finding allegations that defendant sold passcodes to IKS service sufficient to plead a DMCA claim); *DISH Network L.L.C. v. Bolanos*, No. CV 12-03097 DSF (OPx), 2012 WL 5896599, at *1-2 (C.D. Cal. Nov. 21, 2012) (same). The allegations in Nagravision's complaint are also supported by the Metral Declaration that is filed in conjunction with this motion. *See supra* Part I.B.

Accordingly, the first factor weighs in favor of granting Nagravision's motion. *See, e.g.*, *Combat Zone*, 2013 WL 230382, at *5 (finding first factor met where plaintiff claimed copyright

infringement, provided certificate of registration, and listed the IP address of persons purportedly making unauthorized reproductions of the copyrighted works); *Well Go USA*, 2012 WL 4387420, at *2 (first factor satisfied based upon allegations in complaint concerning copyright infringement and having the IP address of the alleged infringer); *Indigital Sols.*, 2012 WL 5825824, at *2 (first factor satisfied where the complaint stated a claim based upon anonymous defendants' violation of the Computer Fraud and Abuse Act).

B. Nagravision's Subpoenas Are Narrowly Tailored Toward Identifying Defendants

Nagravision is requesting permission to serve subpoenas on the ISPs that are assigned the IP addresses of CW Servers 1-7. Defendant Does 1-7 are the customers of the ISPs, and as shown above are using the infrastructure and services provided by these ISPs to retransmit Nagravision's control words to end users without authorization.

Nagravision's proposed subpoena to each of the three ISPs has been filed with the Court. (Metral Decl. ¶ 14, Ex. 18.) Request Nos. 1-3 call for an account profile or other record that shows the name and contact information of each customer, account applications, and statements. (*Id.* ¶ 15.) The foregoing is relevant for purposes of identifying the persons operating CW Servers 1-7. *See Nagravision SA v. Zhuhai Gotech Intelligent Tech. Co.*, No. 4:15-cv-00403, Dkt. 11 (S.D. Tex. May 27, 2015) (granting Nagravision's motion to take expedited discovery of account records in similar case to identify persons operating IKS service) (attached at Metral Decl. Ex. 19); *Indigital Sols.*, 2012 WL 5825824, at *3 (authorizing expedited discovery of account records for purposes of identifying the infringer); *Well Go USA*, 2012 WL 4387420, at *4 (same). However, based on Nagravision's experience in similar cases, these account records will likely be inadequate, standing alone, to identify the persons responsible for CW Servers 1-7. (Metral Decl. ¶ 15.)

There were a number of instances where Nagravision obtained authorization from a court to discover the name and contact information of a customer responsible for a server used as part of an IKS service, and the information provided by the ISP in response to the order was fabricated and not associated with a real person. (*Id.* ¶ 16.) As an example, in one proceeding Nagravision was granted a disclosure order from the Court of Paris instructing an ISP to provide Nagravision

with information concerning a customer involved in an IKS server operation. (*Id.*) The account records produced by the ISP identified the customer as having the first name "Frank" and the last name "Stein" – an apparent reference to the fictional character, Frankenstein. (*Id.*) The mailing address listed for this "Frank Stein" was not a valid address, and the email address and telephone number in the ISP's account records also did not correspond with the real customer. (*Id.*) This is one example of a pay-television pirate providing their ISP with a false name and contact details to hide their true identity. (*Id.*)[1]

Accordingly, Nagravision needs to discover information from the ISPs that cannot be easily faked, and which if necessary will provide the basis for further discovery to identify the persons responsible for CW Servers 1-7. (*Id.* ¶ 17.) Billing information is an example. (*Id.*) Request No. 4 of the subpoenas calls for documents identifying the financial account used to pay the ISPs. (*Id.*) With this information, Nagravision can request discovery from the financial institution and obtain the name and contact information of the account holders paying the ISPs to host CW Servers 1-7. (*Id.*) The billing information may also show that more than one person is involved in operating or otherwise responsible for these servers. (*Id.*) Request No. 4 is therefore appropriate. *See Zhuhai Gotech*, No. 4:15-cv-00403, Dkt. 11 at 1 (authorizing Nagravision to obtain payment records from ISPs as part of order granting motion for expedited discovery).

By the same token, Request No. 5 calls for communications between the ISPs and persons in control of CW Servers 1-7, such as account set-up correspondence and customer support tickets. (Metral Decl. ¶ 18.) The persons operating the servers, even if false information was provided when creating the accounts, may inadvertently identify themselves in communications with the ISPs. (*Id.*) The communications may also show there is more than one person operating the servers. (*Id.*) The requested communications are not personal in nature, and are an appropriate subject for discovery

[1]*See also Zhuhai Gotech*, No. 4:15-cv-00403, at Dkt. 10-4 ¶ 6, Ex. 4 (attaching subpoena-related correspondence received from an ISP in a similar case, stating "[a] lot of our customers don't even use real names or valid addresses … 'We don't care as long as the money's there'").

to identify Defendants. *See Zhuhai Gotech*, No. 4:15-cv-00403, Dkt. 11 at 2 (granting expedited discovery of account set-up correspondence and support tickets from ISPs).

Separately, the communications sought in Request No. 5 are relevant to the extent that the person assigned one or more of CW Servers 1-7 is a reseller, meaning that the reseller's customer is likely the responsible Defendant. (Metral Decl. ¶ 19.) By example, in the *Zhuhai Gotech* case, Nagravision received account records and payment information from an ISP in the United States in response to a subpoena, showing that the IKS server was assigned to a reseller in China. (*Id.*) The support tickets produced by the ISP, however, contained information identifying the reseller's customer actually operating the server. (*Id.*) Nagravision amended the complaint and named that customer as a defendant. (*Id.*)

Request No. 6 of the subpoenas calls for an electronic image of CW Servers 1-7. (*Id.* ¶ 20.) The server images should include logs of the IP addresses that accessed the servers. (*Id.*) In the IP address logs, Nagravision expects to find instances where the operators of the servers, marked by their own personal IP address, accessed the servers to install or upgrade the software, manage the administration console, or otherwise maintain these servers. (*Id.*) By issuing discovery to the ISP that assigned the IP address, Nagravision may identify the persons operating CW Servers 1-7 by name. (*Id.*) The logged IP addresses are similar to the billing records requested above in that the persons operating the servers are less likely to fabricate this information. (*Id.*) Server images aimed at uncovering IP addresses used by persons that operate CW Servers 1-7 are an appropriate subject for expedited discovery. *See Zhuhai Gotech*, No. 4:15-cv-00403, Dkt. 11 at 2 (authorizing Nagravision to obtain server images from ISPs); *see also Indigital Sols.*, 2012 WL 5825824, at *3-4 (allowing expedited discovery of logged IP addresses for purposes of identifying defendants).

The server images sought in Request No. 6 of the subpoenas is also relevant if CW Servers 1-7 are assigned to a reseller. (Metral Decl. ¶ 21.) For example, in *Zhuhai Gotech*, server images provided by an ISP allowed Nagravision to identify the control word sharing software running on the IKS server. (*Id.*) Certain software files were configured such that an alert message was sent to specified email addresses in the event the IKS server malfunctioned. (*Id.*) The email addresses

corresponded with employees of the defendants that were subsequently named in that case. (*Id.*) The foregoing further demonstrates the relevance of the server images for purposes of identifying the persons responsible for CW Servers 1-7. (*Id.*)

Finally, Request No. 7 of the subpoenas calls for the ISPs to capture network traffic to and from CW Servers 1-7 for a limited period of time. (*Id.* ¶ 22.) Nagravision requests this connection traffic because it has experienced cases where data on an IKS server was encrypted by the server operator in order to prevent attempts by Nagravision to discover their information, such that real-time analysis of the servers was the only way to obtain the requested material. (*Id.*)

For example, in November 2012, Nagravision obtained an order from the High Court of Chancery, United Kingdom, requiring that an ISP provide information on its customers involved in operating an IKS service. (*Id.* ¶ 23.) The ISP produced to Nagravision a virtual machine that emulated the ISP's servers. (*Id.*) Nagravision discovered that the control word sharing software was stored in and ran from a file the customer encrypted and disguised as a Microsoft Windows system file. (*Id.*) The encryption prevented Nagravision from analyzing data in the file, which if available may have assisted Nagravision in identifying the responsible customer. (*Id.*) If data on CW Servers 1-7 is encrypted, the server images will be inadequate and instead Nagravision must review connection traffic captured while the servers are active to discover the IP address used by the persons managing the servers. (*Id.*)

Connection traffic is also required to identify the source of the Nagravision control words transmitted through CW Servers 1-7. (*Id.* ¶ 24.) The servers are believed to receive control words from additional servers connected to smart cards that are activated on subscription accounts held with pay-television providers using Nagravision's security technology. (*Id.*) To date, Nagravision has not been able to identify the IP addresses of the servers from which the control words originate. (*Id.*) Connection traffic will enable Nagravision to identify the source of the Nagravision control words transmitted through CW Servers 1-7, and in turn issue additional discovery to uncover the persons operating the servers. (*Id.*) Request No. 7 of the subpoenas is therefore appropriate. *See*

Zhuhai Gotech, No. 4:15-cv-00403, Dkt. 11 at 2 (allowing Nagravision to issue subpoenas to ISPs for server connection traffic).

In sum, Nagravision's subpoenas are based on specific IP addresses located as part of its investigation of Defendants' IKS service, and the information sought from the ISPs is focused at identifying Defendants, such that the second factor weighs in favor of granting this motion. *See Zhuhai Gotech*, No. 4:15-cv-00403; *Combat Zone*, 2012 WL 230382, at *5 (holding that proposed subpoenas for "'ISPs to produce any and all documents and/or information sufficient to identify the user or users' of the IP addresses" were sufficiently specific to satisfy the second factor).[2]

C. Nagravision's Subpoenas Are Necessary To Identify Defendants

The third and fourth factors look at whether there is an alternative means for obtaining the information requested in the subpoena, and whether that information is necessary to advance the claim. *Turner*, 2013 WL 2147515, at *3. Nagravision conducted a thorough investigation and thus far is unable to identify Defendants. (Metral Decl. ¶ 13.) Nagravision does not have a means of identifying Defendants other than subpoenas to the ISPs. (*Id.*) And, Nagravision must identify Defendants to move forward with this case. The third and fourth factors therefore weigh in favor of granting Nagravision's motion for expedited discovery. *See, e.g., Zhuhai Gotech*, No. 4:15-cv-00403, Dkt. 11; *Combat Zone*, 2013 WL 230382, at *5 (finding third and fourth factors satisfied because subpoena to ISP was necessary to identify unknown infringer and case could not proceed until the defendant was identified and served); *Well Go USA*, 2012 WL 4387420, at *2 (reaching same conclusion). In fact, two of the three ISPs that Nagravision is requesting leave to subpoena, Sharktech and DataShack, previously complied with a similar subpoena in *Zhuhai Gotech*, and those responses assisted Nagravision in identifying the responsible customers and naming them as defendants in that case. (Metral Decl. ¶ 14.)

[2]*See also Nagravision SA v. iWeb Techs., Inc.* (20 June 2014), Montreal No. 500-17-081938-147 (Q.C.C.S.) (allowing discovery equivalent to that requested here and in the *Zhuhai Gotech* case) (attached at Metral Decl. Ex. 20).

D. Nagravision's Subpoenas Will Not Violate Defendants' Expectation Of Privacy

The final factor considers the effect the discovery might have on Defendants' reasonable expectation of privacy. *Turner*, 2013 WL 2147515, at *3. Defendants, as established above, are operating an IKS service that facilitates others to circumvent the Nagravision security technology and receive programming provided by Nagravision's customer without authorization. *See supra* Part I.B. Defendants cannot rely upon a First Amendment right of privacy to prevent Nagravision from discovering their participation in this infringing operation. *See West Coast Prods., Inc. v. Does 1-351*, No. 4:12-cv-00504, 2012 WL 2577551, at *4 (S.D. Tex. July 3, 2012) (denying Doe defendant's attempt to prevent ISP from disclosing his identity on privacy and free speech grounds, finding that if "anonymity is used to mask copyright infringement or to facilitate such infringement by others, the First Amendment is no protection"); *see also Dallas Cowboys Cheerleaders, Inc. v. Scoreboard Posters, Inc.*, 600 F.2d 1184, 1188 (5th Cir. 1979) ("The first amendment is not a license to trammel on legally recognized rights in intellectual property.").

Furthermore, with regard to the specific information requested from the ISPs, Defendants will be allowed a fair opportunity to object to Nagravision's subpoenas. *See infra* Part IV. At that time, Defendants are free to seek a protective order from the Court if they believe any part of the information requested from the ISPs is deserving of additional safeguards. Given the availability of a protective order, the expectation of privacy factor weighs in favor of granting this motion for expedited discovery. *See, e.g., Combat Zone*, 2013 WL 230382, at *5 (holding that subscriber's expectation of privacy would be upheld by protective order and therefore the last factor supported issuance of subpoena to ISP); *Well Go USA*, 2012 WL 4387420, at *2 (same).

E. Evidence Preservation Concerns Further Justify Nagravision's Subpoenas

There is good cause to allow expedited discovery where the evidence sought is in danger of destruction or loss. *See, e.g., St. Louis Group*, 275 F.R.D. at 240-41 (noting that "courts have granted expedited discovery requests when there is some showing of irreparable harm that can be addressed by limited, expedited discovery," and listing examples such as cases where there was a risk of destruction or loss of evidence of infringement); *Indigital Sols.*, 2012 WL 5825824, at *3-

4 (allowing expedited subpoenas and taking into account the information identifying the infringer may only be preserved for a limited period of time).

Here, there is a genuine risk that Defendants, once notified of this lawsuit, will attempt to alter or delete data from CW Servers 1-7, or otherwise relocate their IKS services to new servers and thus force Nagravision to restart its investigation and legal action anew. (Metral Decl. ¶ 25.) Nagravision experienced similar behavior by IKS server operators under analogous circumstances, including in the *Zhuhai Gotech* case previously filed in this Court. (*Id.* ¶¶ 26-27 [listing additional instances where IKS server operators moved servers after Nagravision sought assistance from their ISP].) In fact, courts have observed that pay-television pirates, like Defendants, are predisposed to destroy or hide evidence of their wrongdoing once confronted with legal action. *See, e.g., DISH Network L.L.C. v. Howard*, No. 3:13-cv-01136, Dkt. 10 at 6 (N.D. Ind. Nov. 4, 2013) (stating "pirates are often the type of defendant who would destroy or hide evidence when provided notice of the claims against them"); *DISH Network L.L.C. v. Carillo*, No. 3:09-cv-01428, Dkt. 11 at 6 (D. Conn. Sept. 21, 2009) (finding "telecommunications pirates are the types of defendants who would violate court orders," and sealing the case "to address the risk that evidence of illegal activity will be destroyed"); *DISH Network L.L.C. v. Hipps*, No. 1:08-cv-00357, Dkt. 16 at 6 (W.D.N.C. Aug. 5, 2008) (noting "the well-known tendency of alleged pirates to vanish with key evidence as soon as they get wind of impending legal action") (orders attached at Metral Decl. Exs. 21-23.)

The relocation of Defendants' IKS service from CW Servers 1-7 to new servers presents a serious threat of harm to Nagravision because certain information requested in the subpoenas will become unavailable. (Metral Decl. ¶ 29.) Nagravision will be unable to obtain connection traffic, which is important for identifying IP addresses used by Defendants and the IP addresses of servers from which Nagravision's control words originate. (*Id.*) Defendants may also alter or delete data from their servers, including the logged IP addresses and the control word sharing software running on the servers, which are valuable for purposes of identifying Defendants. (*Id.* ¶ 30.) Defendants may also destroy evidence required for the merits of Nagravision's claim, such as the control word

sharing software and information on the number of end users that obtained control words from the servers, the latter of which is relevant for quantifying damages. (*Id.*)

To sum it up, there is additional good cause to grant Nagravision's motion for expedited discovery because the information needed to identify Defendants and other evidence necessary to establish liability and damages may not be available once Defendants are notified of this action. [3]

IV. CONCLUSION

For at least these reasons, the Court should grant Nagravision's motion for leave to take limited discovery prior to the Federal Rule of Civil Procedure 26(f) conference for the purpose of identifying Defendant Does 1-7. A proposed form of order has been submitted, which sets forth a three step approach whereby the ISPs first preserve the information requested in the subpoenas, next notify the responsible customers and each have an opportunity to object to the subpoena or move for a protective order, and finally the ISPs produce the information to Nagravision after any challenges are resolved. This strikes the appropriate balance between preservation of the necessary evidence and providing the ISPs and Defendants the ability to be heard. Nagravision also agrees to reimburse the ISPs for costs reasonably incurred in responding to the subpoenas, which further reduces any burden to them.

Dated: July 14, 2017

Respectfully submitted,

HAGAN NOLL & BOYLE, LLC

s/ Chad M. Hagan
Chad M. Hagan (attorney-in-charge)
Texas Bar #24036700
S.D. Tex. Bar #36439
Two Memorial City Plaza
820 Gessner, Suite 940
Houston, Texas 77024
Telephone: (713) 343-0478
Facsimile: (713) 758-0146
chad.hagan@hnbllc.com

[3] *See Zhuhai Gotech*, No. 4:15-cv-00403, at Dkt. 10-4 ¶¶ 3-4, Exs. 1-2 (addressing two instances where Nagravision subpoenaed an ISP for a server image and connection traffic, and in response was informed that the server was no longer in use and the hard drive had been wiped clean).

Timothy M. Frank (of counsel)
Texas Bar #24050624
S.D. Tex. Bar #614705
timothy.frank@hnbllc.com

Attorneys for Plaintiff Nagravision SA